CLAIMS

1. An information encrypting transmission and reception method in an information transmission and reception network composed of a plurality of senders and receivers having computers being connected and communicating each other via a web network and a data center having a server computer for receiving electronic key data of bit data formed by the senders and receivers and personal data such as address corresponding to each electronic key data to register the serer computer and certifying the senders and the receivers with each personal data, comprising:

by one of the senders, firstly decrypting bit data of original information such as plaintext to be transmitted to one of the receivers by performing an exclusive OR operation in use of the bit data of the registered electronic key of the sender and transmitting the firstly encrypted data attached with personal data of the sender and the receiver to the receiver;

by the server computer of the data center, decrypting the bit data of the electronic key of the sender by performing an exclusive OR operation on the transmitted firstly encrypted bit data in use of bit data of the key data of the sender certified with the personal data of the sender, secondly encrypting the decrypted data by performing an exclusive OR operation the in use of bit data of the registered electronic key of the receiver

certified with transmitted personal data of the receiver so as to form secondly encrypted bit data, and transmitting the secondly encrypted bit data to the receiver; and

by the receiver, receiving the secondly encrypted bit data from the data center, and decrypting the secondly encrypted bit data in to the original information such as plaintext by performing an exclusive OR operation in use of bit data of the electronic key of the receiver.

2. An information encrypting transmission and reception system in an information transmission and reception network composed of a plurality of senders and receivers having computers being connected and communicating each other via a web network and a data center having a server computer for receiving electronic key data of bit data formed by the senders and receivers and personal data such as address corresponding to each electronic key data to register the server computer and providing the data only to a person who is certified his or her validity in use of the registered data as certification data, comprising:

providing a sender server computer for transmitting and receiving data of the senders and a receiver server computer for transmitting and receiving data of the receivers that are connected to the web network;

firstly encrypting bit data of original information such as plaintext to be transmitted from one of the senders to one

of the receivers by performing an exclusive OR operation in use of bit data of electronic key of the sender and transmitting the firstly encrypted bit data attached with personal data of the receiver to the sender server computer;

by the sender server computer, receiving bit data of the electronic key of the receiver by submitting personal data of the receiver to the data center, secondly encrypting the firstly encrypted bit data by performing exclusive OR operation in use of received bit data of the electronic key of the receiver, and transmitting the secondly encrypted bit data attached with personal data of the sender and the receiver to the receiver server computer;

by the receiver server computer, receiving the secondly encrypted bit data, receiving bit data of the electronic key of the sender by submitting personal data of the sender to the data center, thirdly encrypting the secondly encrypted bit data by performing exclusive OR operation in use of received bit data of the electronic key of the sender, and informing the receiver about the reception of the thirdly encrypted bit data or transmitting the thirdly encrypted bit data to the receiver; and

by the receiver, obtaining the original information such as plaintext from the sender by performing an exclusive OR operation on the thirdly encrypted bit data in use of the bit data of the electronic key of the receiver.

3. The information encrypting transmission and reception method according to one of Claims 1 and 2, wherein the original information such as plaintext is preliminary encrypted by performing an exclusive OR operation on at least each bite of the original information in use of random number bit data in advance of firstly encrypting of the original data in use of bit data of the electronic key of the sender.

4. The information encrypting transmission and reception method according to Claim 3, wherein bit data of the random number and/or electronic key is a password random number of the n bit including 6 to 10 digits of 64 bits, a pseudo random number based on the random number, a chaos random number, or a fractal random number.

5. The information encrypting transmission and reception system according to one of Claims 1 to 4, wherein the server computer of the data center uses electronic key data set by each sender and receiver as electronic personal seal data for authentication and as information hiding data for hiding data transmitted and received between the sender and the receiver.

6. The information encryption transmission and reception

system according to Claim 5, wherein
chaos image data or fractal image data is used for the electronic personal seal data and/or the information hiding data.

7. The information encrypting transmission and reception system according to Claim 6, wherein
the image data in Claim 6 is moving image data.

8. The information encrypting transmission and reception system according to one of Claims 2 to 7, wherein
the receiver server computer informs the receiver with an electronic envelop data that encrypted communication document is received.

9. An information encrypting transmission and reception method, comprising:

forming firstly encrypted data (C) by performing an exclusive OR operation on bit data (A) of original information such as plaintext to be transmitted in use of random bit data (B) known to a sender and a receiver;

forming secondly encrypted data (E) by performing an exclusive OR operation on the data (C) in use of bit data (D) of an electronic key obtained only by the sender and receiver;

forming thirdly encrypted data (G) by performing an exclusive OR operation on the data (E) in use of bit data (F)

of an electronic envelop registered by the sender or the receiver; and

transmitting the thirdly encrypted data (G) and the data (F) of the electronic envelop to the receiver.

10. The information encrypting transmission and reception method according to Claim 8, wherein
bit data of the random number, bit data of the electronic key, and bit data of the electronic envelop are registered to the data center or the server computer set as an authenticator so as to be readable only by an valid person.

11. The information encrypting transmission and reception method according to one of Claims 9 and 10, wherein
bit data of the random number and/or electronic key is a password random number of the n bit including 6 to 10 digits of 64 bits, a pseudo random number based on the random number, a chaos random number, or a fractal random number.